METHODOLOGICAL APPROACH TO THE SENSITIVITY ANALYSIS OF FAILURE EFFECTS IN MODERN DIGITAL I&C SYSTEMS

Christian Mueller, Joerg Peschke, Ewgenij Piljugin, Dagmar Sommer
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH
Schwertnergasse 1, 50667 Cologne, Germany
christian.mueller@grs.de; joerg.peschke@grs.de; ewgenij.piljugin@grs.de; dagmar.sommer@grs.de

ABSTRACT

Modern I&C systems of nuclear power plants increasingly use digital equipment, software-based applications for I&C functions and different types and topologies of communication networks as well. The structure, operation and communication of digital safety-related I&C systems are strongly influenced by the implemented automatic fault detection and fault treatment procedures as barriers against failure propagation. Thus, these I&C systems can change their operating states automatically during the operation time, e.g. due to the detection and correction of certain failure types. Reasonably because of these dynamic properties of digital I&C systems the use of classical fault tree and event tree methods solely for the reliability analysis of modern I&C systems is less suitable. These methods basically apply static models and do not consider the temporal changes of the operating state of the I&C system or equipment appropriately.

In this paper, a recently developed approach for the sensitivity analysis of digital I&C systems will be introduced that allows to investigate the dynamic behavior of such systems in cases of internal faults and to quantify the effects on the system reliability. The development and testing of the analysis methodology is carried out using models of generic I&C systems with different typical architectures of stepwise increased complexity.

Key Words: Digital I&C, FMEA, FTA, Markov, sensitivity analysis

1 INTRODUCTION

The developed methodology for the sensitivity analysis of digital I&C systems is a graded approach and based on the application of failure mode and effect analyses (FMEA) [1], fault tree analyses (FTA) [2] and semi-Markov processes [3]. The analysis comprises several models with stepwise increased complexity of the I&C architecture and of the deployment of different fault tolerant features.

In the next section, the simplified model systems used in this study are explained more detailed and the methods, which are used, are briefly explained in the following section. Subsequently, some preliminary results are presented.

The authors want to acknowledge the support provided by the German Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety for funding the GRS development of the methodological approach to the sensitivity analysis of failure effects in modern digital I&C systems in the frame of the R&D project 3615R01343.

2 MODEL SYSTEMS

A series of simple to more complex model systems is used to develop and perform the sensitivity analysis. Without redundancy or diversity, the model systems would have a simple linear structure of signal processing and would consist of an acquisition unit (AU) on the acquisition level, a processing unit

(PU) on the processing level, a voting unit (VU) on the control level and additional an analog logic (AL) (see Figure 1).

On the acquisition level the measured values (e.g. pressure) are recorded in redundant acquisition units (AUs), which digitize and subsequently transmit these values as data telegrams via the communication network to the next level (processing level). The transmission of each signal is marked with a flag. If a signal is detected as faulty on this level, the flag is set to “1” (self-signaling failure (“SF”)). If the flag is set to “0”, it can be either a true signal (“OK”) or a non-self-signaling failure (“NSF”).

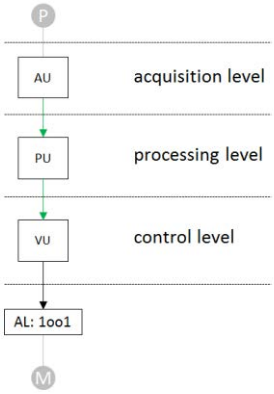

Figure 1. Basic structure of the model systems.

On the processing level the digitized measured values are evaluated in processing units (PUs). The valid signals (flag “0”) from the AUs are sorted in ascending order and the second maximum is selected from them. If some input signals have self-signaling failures (flag “1”), the second maximum is chosen only from the remaining valid signals (flag “0”). If all but one signal coming from the AUs are flagged with “1”, the remaining input signal is used directly as “second” maximum.

The second maximum is then compared with a limit value and, if necessary, a binary control signal (“1”-“ON” or “0”-“OFF”) is generated and forwarded to the next level (control level). Again, the detected failures of the PUs or of the communication network between the PUs and voting units (VUs) are marked with a flag “1” and are therefore recognized as invalid signals.

In the VUs, the binary signals of the previous level are evaluated by means of an n-out-of-m voting and, if necessary, a control signal for a component (e.g. motor) is formed. If only one or two valid inputs are available, the VUs internally switch to a 1-out-of-2 voting so that a single valid signal is sufficient to form a trigger signal. The output signals of the VUs to the analog logic (AL) do not contain error detection information, but self-signaling failures are reported and can be repaired if necessary.

The AL again performs an n-out-of-m voting (as there may be several VUs in an individual model system) and then passes the control signal to the component.

In addition, the following assumptions are made:

- The communication between units (“computers”) is carried out via networks. It is assumed that all hardware failures in the communication networks are always detected and they are therefore always self-signaling. For this reason, the failure rates of the communication paths (for example, between AUs and PUs) are taken into account directly in the failure rates of the corresponding signal-sending components (for example, self-signaling failures of AUs).
- Non self-signaling failed AUs output the minimum possible value.

- Non self-signaling failed PUs output a logical “0”.
- Failed VUs output a logical “0”.
- The software of the AUs, PUs and VUs is not modeled explicitly so far and the considered failure rates were determined initially only by the possible hardware failures [2].
- Measuring devices, power supplies and interfaces of the I&C system are not explicitly taken into account in the models.

Until now, the following model systems have been used for development and validation:

- A222: 2 VUs, 2 PUs and 2 AUs (see Figure 2)
- A133: 1 VU, 3 PUs and 3 AUs
- A333: 3 VUs, 3 PUs, 3 AUs
- A133A133: Two systems of the type A133 in parallel (see Figure 5 (a))
- A133B133: Two systems of the type A133 (with diverse components - “A”, “B”) in parallel (see Figure 5 (b))
- A2MC(1)33: 2 VUs (each with 1 sub-unit (Master-Checker)), 3 PUs and 3 AUs
- A2MC(2)44: 2 VUs (each with 2 sub-units (Master-Checker)), 4 PUs and 4 AUs (see Figure 6)

3 METHODS

First of all, an FMEA was carried out for all model systems. Since each signal from each unit of a level (e.g. all AUs) is transmitted to each unit of the subsequent level (e.g. to all PUs, Figure 2) within all model systems, the results of the FMEA can be presented in separated tables for each level.

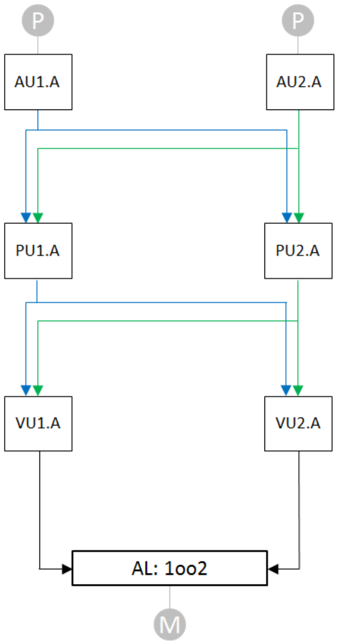

Figure 2. The model system A222.

As an example, table I shows the possible signals from the analog logic (AL) of the model system A222 (Figure 2) in case of demand. As the AL is not part of the digital I&C system, the signals to the component ("motor") can only be either correct ("1"-"OK") or failed ("0"-"NSF"). The failure of the AL can be caused by the AL itself or by the signals coming from the VUs. The signals, which are coming from the VUs (see table II), on the other hand, can be either correct ("1, OK", flag "0"), self-signaling failed ("0, SF", flag "1") or non-self-signaling failed ("0, NSF", flag "0"). This description can be transferred analogously to the other two levels (PUs, AUs).

Table I. Analog Logic Output Signals.

Analog Logic (AL)
Out, Quality
1, OK
0, NSF

Table II. Output Signals of VUs and their Impact on the AL.

VU1.A		VU2.A		AL
Out, Quality	**Flag**	**Out, Quality**	**Flag**	**M starts on demand**
1, OK	0	1, OK	0	yes
0, SF	1	1, OK	0	yes
1, OK	0	0, SF	1	yes
0, NSF	0	1, OK	0	yes
1, OK	0	0, NSF	0	yes
0, SF	1	0, SF	1	no
0, SF	1	0, NSF	0	no
0, NSF	0	0, SF	1	no
0, NSF	0	0, NSF	0	no

The results of the FMEA can be directly translated into a fault tree. For example, the figures 3 and 4 show the sections of the fault tree for the model system A222 which correspond to the tables I and II.

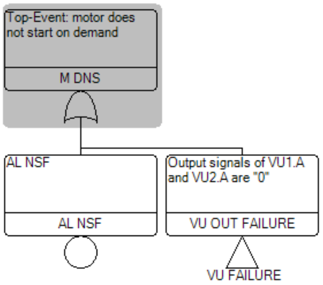
Top-Event: motor does not start on demand
M DNS
AL NSF
AL NSF
Output signals of VU1.A and VU2.A are "0"
VU OUT FAILURE
VU FAILURE

Figure 3. Top-Event in the fault tree for the model system A222 ("motor does not start on demand").

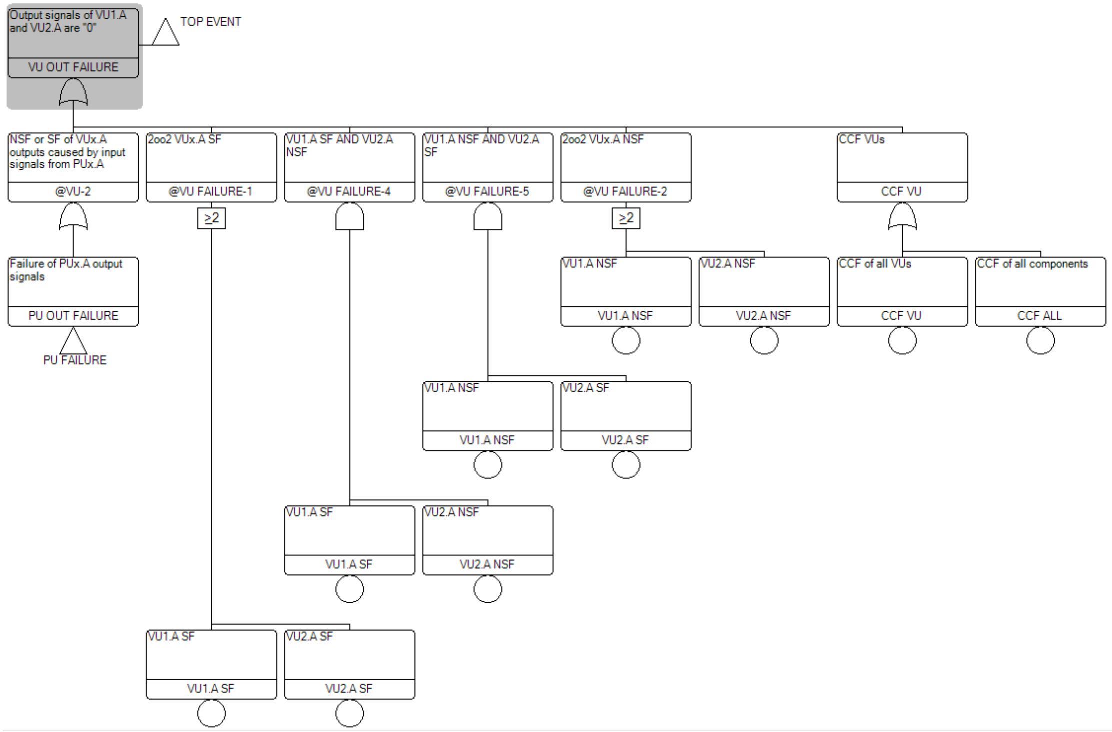

Figure 4. Section of the fault tree for the model system A222. which describes the signals coming from the VUs (compare to table II).

At present, the analyses are extended using semi-Markov processes. Semi-Markov processes describe the model systems by means of (time-dependent) transition graphs, which elements represent the overall state of the system and are connected with transition arrows with certain transitional probabilities. The work on this is ongoing.

4 FIRST RESULTS

Although the project is still ongoing, there are already first interesting results. Figure 5 shows the model systems A133A133 and A133B133. Both model systems are essentially the same, but differ in terms of diversity ("A" and "B"). In addition, figure 6 shows the (highly redundant) model system A2MC(2)44. For the analysis, it was assumed that self-signaling failures are repaired within eight hours and that non-self-signaling failures are detected in weekly rotating inservice inspections of the redundancies and then repaired within eight hours, too.

For the analysis it has been also assumed, that the failure rates for the same kind of units (AUs, PUs or VUs) is the same in all model systems, but common cause failures (CCF) only affect units within each diversity ("A" or "B"). The failure rates for the different kind of units (AUs, PUs, VUs, AL) have been taken from [4].

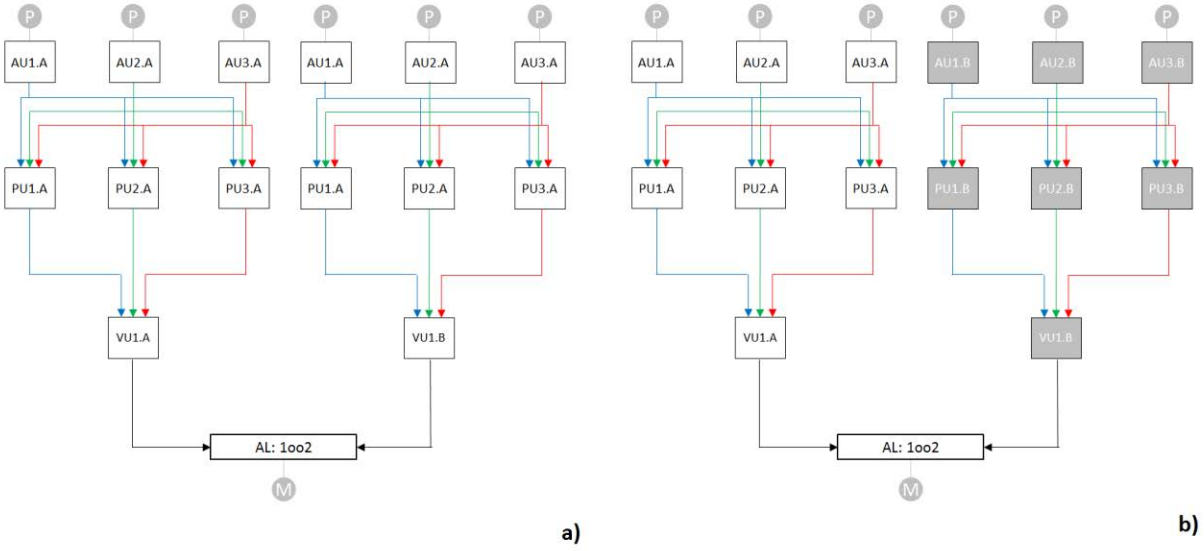

Figure 5. Model systems A133A133 (a) and A133B133 (b).

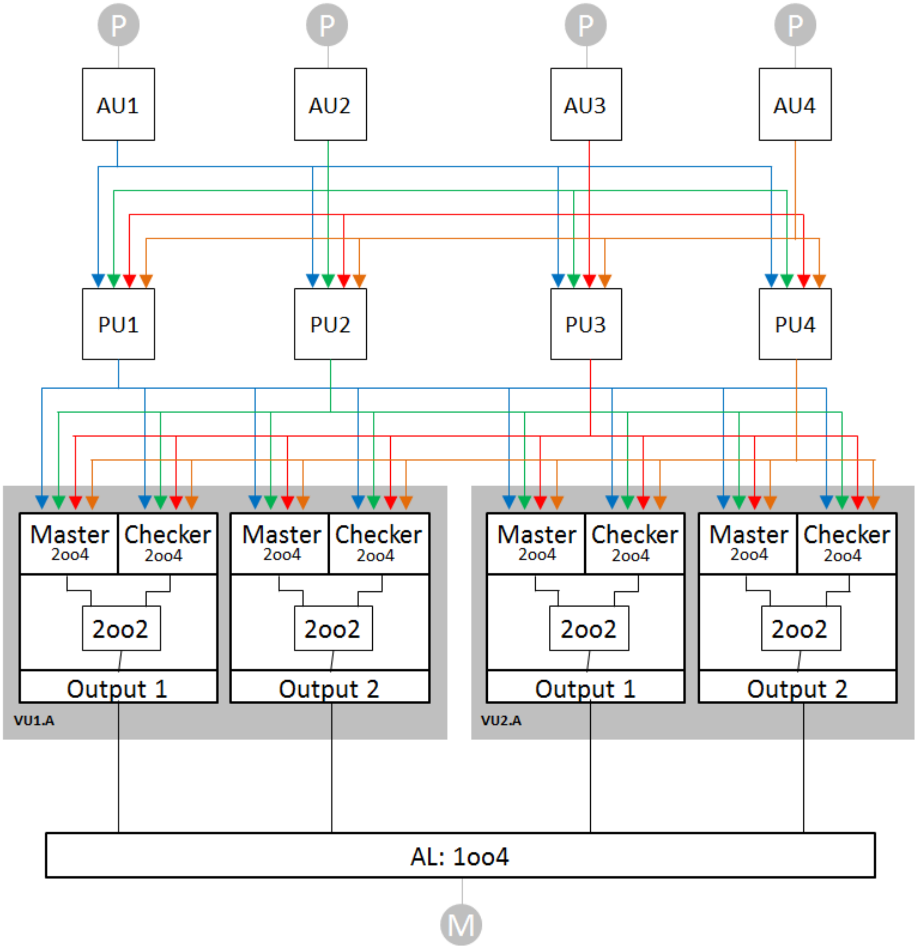

Figure 6. Model system A2MC(2)44 (one diversity (A) with 2 VUs (each with 2 Sub-Units (Master-Checker)), 4 PUs and 4 AUs).

The figures 7 and 8 display the expected number of failures and the failure probability (Q(t)) as a function of time for the three model systems A133A133 (a), A133B133 (b) and A2MC(2)44 (c) acquired with RiskSpectrum PSA [5]. As clearly visible, increasing the grade of redundancy has a smaller effect on the reliability of the system than adding diversity. The reliability of A133B133 is more than an order of magnitude higher than that of A133A133. Even adding a much higher rate of redundancy (as in A2MC(2)44) does not lead to better reliability in comparison with A133A133 (Figure 7 and Figure 8).

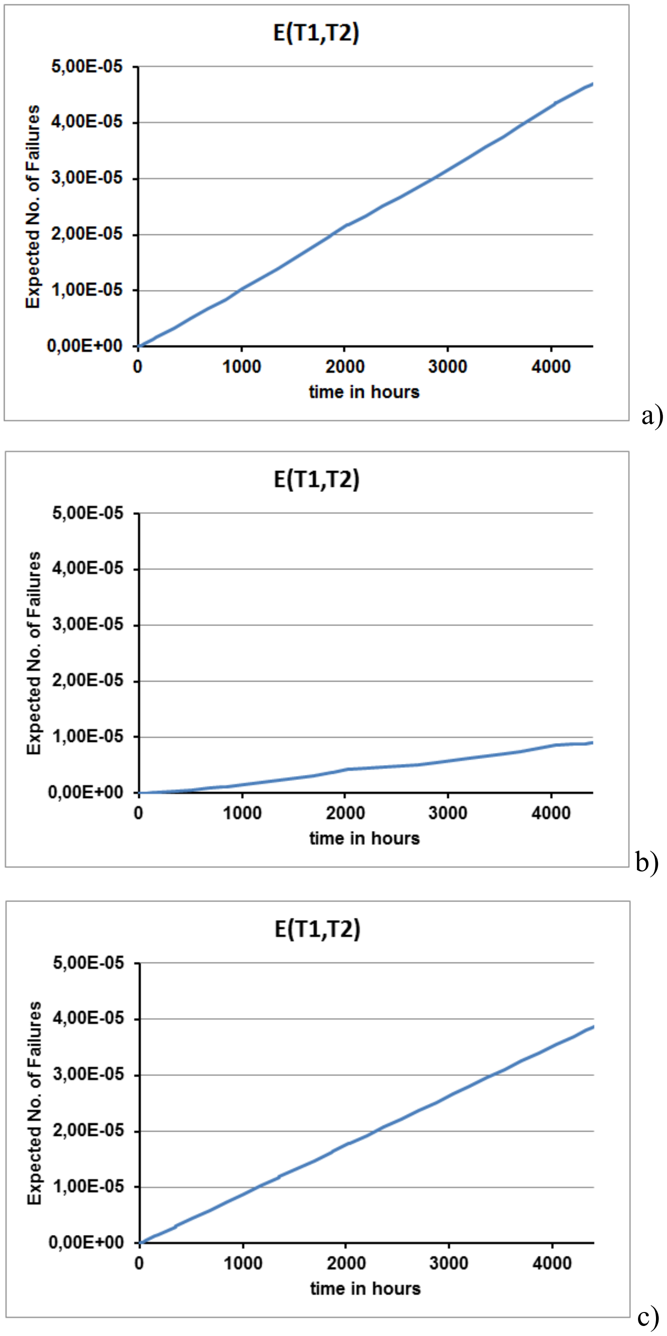

Figure 7. Expected number of failures for the model systems A133A133 (a), A133B133 (b) and A2MC(2)44 (c) as a function of time in hours.

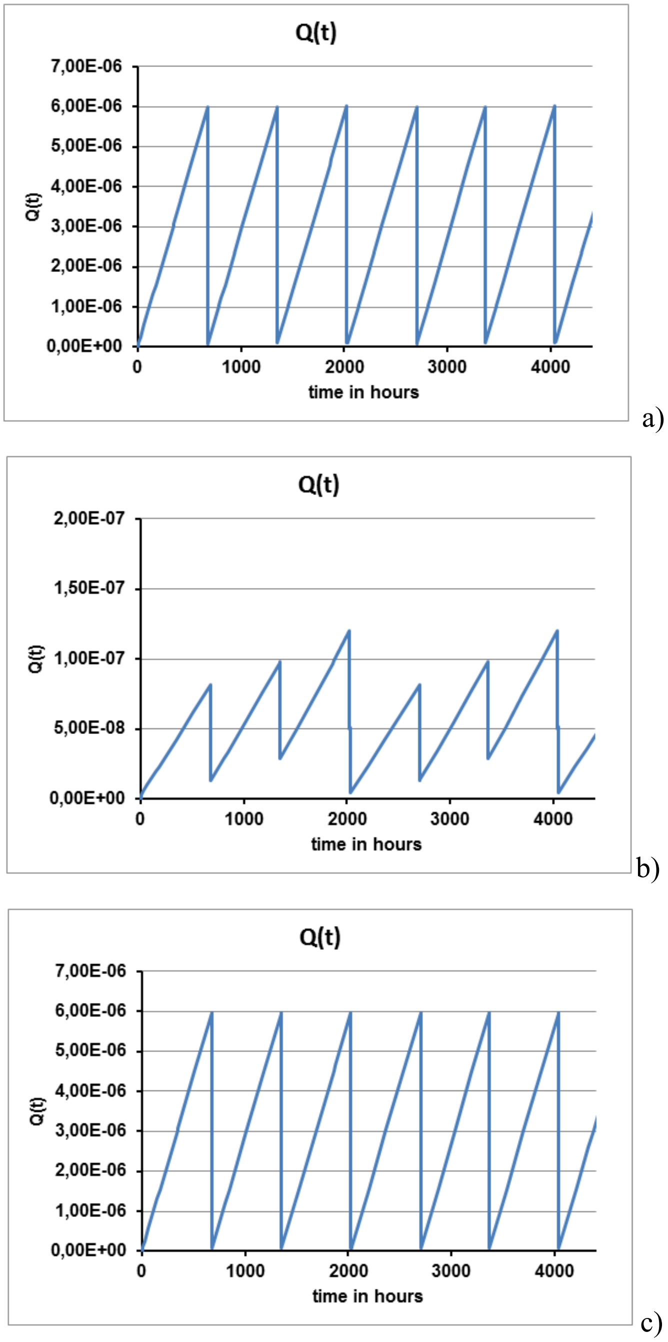

Figure 8. Failure probability (Q(t)) for the model systems A133A133 (a), A133B133 (b) and A2MC(2)44 (c) as a function of time in hours. Note that the graph b) is scaled differently.

5 CONCLUSIONS

At present a methodological approach is being developed for the sensitivity analysis of failure effects on digital I&C systems. With a combination of failure mode and effect analyses (FMEA), fault tree analyses (FTA) and semi-Markov processes, different model systems with increasing complexity are investigated.

Although the project has not yet been finalized, the first promising results are already available. Thus, the effect of a higher diversity can already be compared with the effect of a mere increase in redundancy. Due to the high influence of common cause failures (CCF) on the reliability of I&C systems, a significant increase of the reliability can only be achieved by adding diversity at a certain degree of redundancy.

The next step will be the combination of the FTA with semi-Markov processes and the application of the complete methodology on all model systems. Through the variation (sensitivity analysis) of different I&C architectures and parameters (e.g. which describe CCF), the influence of these architectures and parameters on the reliability of the I&C systems will be determined. Further research work could deal with the application of the method to a more complex yet more realistic I&C system.

In conclusion, it can be noted that the developed methodology for the sensitivity analysis presented in this paper can support the verification and validation of digital I&C systems regarding potential safety deficiencies in design and operation even at an early stage.

6 REFERENCES

1. "Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)", *IEC 60812:2006* (2006)
2. "Fault Tree Handbook", U.S. Nuclear Regulatory Commission, *NUREG-0492* (1981)
3. M. Röwekamp, W. Faßman, W. Frey, L. Gallner et al., „Development and Test Application of Methods and Tools for Probabilistic Safety Analyses", GRS, *GRS-A-3558* (2010)
4. E. Piljugin, J. Märtz, H. Heinsohn, W. Frey, „Anpassung und Erprobung von Methoden zur probabilistischen Bewertung digitaler Leittechnik", GRS, *GRS-A-3258* (2004)
5. RiskSpectrum PSA, Lloyd's Register Consulting - Energy AB, Sweden (http://www.riskspectrum.com/)